



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/820,673

04/08/2004

James M. Alkove

MSFT-2867/306926.2

8031

41505

7590

11/21/2006

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)

CIRA CENTRE, 12TH FLOOR

2929 ARCH STREET

PHILADELPHIA, PA 19104-2891

EXAMINER

SHIFERAW, ELENI A

ART UNIT

PAPER NUMBER

2136

DATE MAILED: 11/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/820,673

Applicant(s)

ALKOVE ET AL.

Examiner

Eleni A. Shiferaw

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 31 July 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. Applicant's amendments and arguments with respect to amended claims 1 and 12, and presently pending claims 1-23 have been fully considered but are moot in view of the new ground(s) of rejection.
2. Double patenting rejection previously made is still maintained based on Applicant's response, on 07/27/2006 page 1 par. 5, to timely file Terminal Disclaimer.
3. The examiner accepts the amendments to claim 7 that is previously rejected under 112, second.

Double Patenting

4. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

5. Claims 1-23 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-16 of copending Application No. 10820666. Although the conflicting claims are not identical, they are not patentably distinct from each other because the application '666 teaches all the claims limitation except the differences that are underlined in the following table as an example:

Instant application 10/820673	Copending application 10/820666
<p>12. A method of delivering content from a source to a sink by way of a computing device, the method comprising:</p> <ul style="list-style-type: none">• an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink;• the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including:• the media base;• a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure	<p>1. A method of delivering content from a source to a sink by way of a computing device, the method comprising:</p> <ul style="list-style-type: none">• an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink;• the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path including:• the media base;• a source trust authority (SOTA) associated with and corresponding to the source, the SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path; and

<p>lockbox connecting the source to the media base and representing the source in the protected media path, <u>decrypting the content from the source if necessary, and translating policy associated with the content from a native format into a format amenable to the policy engine if necessary;</u> and</p> <ul style="list-style-type: none"> • a sink trust authority (SITA) associated with and corresponding to the sink, the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path, <u>encrypting content to be delivered to the sink if necessary, and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink if necessary, whereby the sink receives the content and corresponding policy, decrypts the received content if necessary, and renders same based on the received policy;</u> • the SOTA on behalf of the source establishing trust with respect to the protected media path; • the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path; 	<ul style="list-style-type: none"> • a sink trust authority (SITA) associated with and corresponding to the sink, the SITA acting as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path; • the SOTA on behalf of the source establishing trust with respect to the protected media path; • the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path; • the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path; • the SOTA deciding with regard to the propagated policy that the particular type of <u>action cannot be taken</u> with the content as delivered through the protected media path and informing the media base of a <u>refusal to take such action;</u> • the media base informing the application of the <u>refusal to take the action;</u> • the SOTA recognizing that the <u>refusal</u> may be rectified by way of a particular enabler available to such SOTA and the SOTA providing the particular enabler to the application by way of the media base, the provided enabler including information and methods necessary for the application to obtain data necessary to respond to the <u>refusal;</u> • the application receiving the enabler at an interface thereof by way of the media base, and the
---	---

<ul style="list-style-type: none"> • the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path; • the SOTA deciding whether the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same; • the media base informing the application whether the particular type of action can be taken, and if so the application proceeding by commanding the media base to perform such type of action. <p>19. The method of claim 18 wherein if the <u>policy engine determines that a particular element of the protected media path does not satisfies the policy, the policy engine performs an action selected from a group consisting of refusing such element access to the content and preventing content from being delivered through the protected media path.</u></p>	<p>interface applying a common interaction procedure to run the enabler to obtain the data necessary to respond to <u>the refusal</u>;</p> <ul style="list-style-type: none"> • the application providing the obtained data to the media base and the media base employing the provided data to respond to the refusal; • the SOTA deciding with regard to the propagated policy and based at least in part on the responded refusal that the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same; and • the media base informing the application that the particular type of action can be taken, and the application proceeding by commanding the media base to perform such type of action.
---	---

6. This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

7. The differences between these two applications is that the instant application ‘673 has a broader claim limitation as underlined above and the copending application has narrower claim limitations and a secure lockbox act of decrypting/encrypting the content from the source if

necessary, and translating policy associated with the content from a native format into a format amenable to the policy engine if necessary is not disclosed in '666 of claim limitations. Wherein said action, as described in the disclosure of the instant application, is an allowance and refusal action. The missing refusal action of claim 1 of the instant application is stated on dependent claim 19 of instant application. Regarding secure lockbox of decrypting/encrypting content is also described throughout the disclosure as being using a cryptography method to encrypt and lock contents. Examiner applies, Stefik US 5,715,403 col. and col. 9 lines 58-60 and col. 51 lines 24-31, for the well-known method of cryptography. It would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of locking/encrypting method to secure and protect transmission of contents.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. Claims 1-23 are rejected under 35 U.S.C. 102(b) as being anticipated by Candelore USPN 7,120,250 B2.

Regarding claim 1, Candelore discloses a computing device having instantiated thereon a protected media path for delivering content from at least one source to at least one sink (fig. 1 and col. 4 lines 29-42), the protected media path comprising:

a media base (fig. 1; DRM) providing a protected environment in the computing device (fig. 1 element 104) and including a common infrastructure of core components effectuating processing of content from any particular source (*multiple different TV channels and/or internet web pages... DRM A,... B in a common digital content provider*) and delivering the processed content to any particular sink (fig. 1 element 112 and col. 6 lines 289-33), and also including a policy engine enforcing policy on behalf of each source (col. 4 lines 43-56, col. 1 lines 36-42), the policy corresponding to the content from the source and including rules and requirements for accessing and rendering the content (col. 6 lines 13-28), whereby the media base allows content to flow through the computing device in a protected fashion, and allows for arbitrary processing of the protected content in the computing device (col. 7 lines 41-65; *contents are processed and encrypted before delivering in the content provider system encrypter*);

a source trust authority (SOTA) in the computing device and associated with and corresponding to each source of content (fig. 1 element DRM A, B; *digital right management in the content provider system associated to every TV channel/webpage providers to protect contents*), each SOTA acting as a secure lockbox connecting the source to the media base and representing the source in the protected media path (col. 4 lines 43-56; *connecting encrypted web contents and DRMs*), decrypting the content from the source (col. 6 lines 13-28), and translating policy associated with the content from a native format into a format amenable to the policy engine (fig. 7 elements 746, and 750); and

a sink trust authority (SITA) in the computing device associated with and corresponding to each sink of content (fig. 7 element 722; *each user's usage content information detector/verifier in the DRM content provider system*), each SITA acting as a secure lockbox

connecting the sink to the media base (fig. 7 element 742; *detector/verifier in the DRM content provider system allowing access to the end users from content provider system*) and representing the sink in the protected media path (col. 6 lines 13-29), encrypting content to be delivered to the sink (fig. 6 element 614), and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink, whereby the sink receives the content and corresponding policy, decrypts the received content, and renders same based on the received policy (fig. 7; *when the user tries to access a content, usage rights are translated, and verified in the DRM content provider system to decrypt content based on rights policy data the DRM stored in the system*).

Regarding claim 12, Candelore discloses a method of delivering content from a source to a sink by way of a computing device (fig. 1 and col. 4 lines 29-42), the method comprising:

- an application on the computing device calling to a media base on the computing device with a definition of the content, the source, and the sink (fig. 1 and col. 4 lines 29-56);

- the media base establishing a protected media path based on the defined content, source, and sink to effectuate such delivery, the established protected media path (col. 3 lines 35-59; encrypted communication) including:

 - the media base (fig. 1; DRM);

 - a source trust authority (SOTA) on the computing device and associated with and corresponding to the source (fig. 1 element DRM A, B; *digital right management in the content provider system associated to every TV channel/webpage providers to protect contents*), the SOTA acting as a secure lockbox connecting the source to the media base and representing the

source in the protected media path (col. 4 lines 43-56; *connecting encrypted web contents and DRM's*), decrypting the content from the source (col. 6 lines 13-28), and translating policy associated with the content from a native format into a format amenable to the policy engine (fig. 7 elements 746, and 750); and

a sink trust authority (SITA) on the computing device and associated with and corresponding to the sink (fig. 7 element 722; *each user's usage content information detector/verifier in the DRM content provider system*), the SITA acting as a secure lockbox connecting the sink to the media base (fig. 7 element 742; *detector/verifier in the DRM content provider system allowing access to the end users from content provider system*) and representing the sink in the protected media path (col. 6 lines 13-29), encrypting content to be delivered to the sink (fig. 6 element 614), and translating the policy associated with the content from the format of the policy engine into a format amenable to the sink, whereby the sink receives the content and corresponding policy, decrypts the received content, and renders same based on the received policy (fig. 7; *when the user tries to access a content, usage rights are translated, and verified in the DRM content provider system to decrypt content based on rights policy data the DRM stored in the system*);

the SOTA on behalf of the source establishing trust with respect to the protected media path (col. 6 lines 13-28; *DRM... copy rights protection on behalf of multiple different TV channels/web pages*);

the SOTA upon trust being established with respect to the protected media path propagating policy corresponding to the content to be delivered to the protected media path (fig. 7 element 722, and col. 4 lines 43-56);

the SOTA determining a particular type of action to be taken with the content as delivered through the protected media path (col. 6 lines 13-28; *viewing*);

the SOTA deciding whether the particular type of action can be taken with the content as delivered through the protected media path and informing the media base regarding same (col. 7 lines 41-65 and col. 6 lines 13-28; *deciding to allow/grant access based on usage term... limited time... keeping track of users access and recording and informing usage information to the DRMs of the content provider system*);

the media base informing the application whether the particular type of action can be taken, and if so the application proceeding by commanding the media base to perform such type of action (fig. 7; *authenticating user rights and allow/deny access*).

Regarding claim 2 Candelore discloses the computing device wherein the media base of the instantiated protected media path further includes at least one supplemental component providing additional protected functionality to the computing device (col. 6 lines 13-30 and fig. 7; *copy protection ... expiration... view only Encryption*)

Regarding claim 3 Candelore discloses the computing device further having instantiated thereon a media application selecting the content to be delivered, selecting each source for providing the content by way of the protected media path, if necessary selecting each sink to receive the provided content by way of the protected media path, actuating the media base to arrange the protected media path according to each selected source and each selected sink (fig. 1; *selecting multiple different TV channel providers/web page providers and transmitting protected to end*

users).

Regarding claim 4 Candelore discloses the computing device wherein the media application provides delivery commands to the media base to control delivery of the content from each selected source to each selected sink (col. 4 lines 29-65).

Regarding claim 5 Candelore discloses the computing device wherein the media base prevents the media application from having access to the content delivered within the protected media path (fig. 1 DRMs).

Regarding claim 6 Candelore discloses the computing device wherein the media base prevents the media application from taking any action with respect to the content contrary to the policy corresponding to the content (fig. 7 element 722).

Regarding claim 7 Candelore discloses the computing device wherein each SOTA of the instantiated protected media path allows content thereof to be delivered through the protected media path 39 only if the SOTA is satisfied that the media base, the policy engine thereof, each employed component thereof, and each SITA of the protected media path is trustworthy and has rights to be in contact with the content based on the policy corresponding thereto (col. 6 lines 13-45 and col. 7 lines 41-65).

Regarding claim 8 Candelore discloses the computing device wherein any element can be shown

Art Unit: 2136

to be trustworthy based on a proffer of an acceptable token that vouches for the element (fig. 7 element 746).

Regarding claim 9 Candelore discloses the computing device wherein any element can be shown to be trustworthy based on a proffer of a verifiable digital certificate from an acceptable vouching authority (col. 6 lines 13-29).

Regarding claim 10 Candelore discloses the computing device wherein a trustworthy element is trusted to decide whether same can be in contact with the content based on the policy corresponding thereto and based on whether same can honor the policy corresponding to the content (col. 7 lines 24-65).

Regarding claim 11 Candelore discloses the computing device wherein a trustworthy element is trusted to respond truthfully to a rights-based query from another element (col. 7 lines 24-65).

Regarding claim 13 Candelore discloses the method wherein the media base establishing the protected media path comprises the media base selecting core components thereof that are to handle and operate on the content while being delivered through the protected media path, the core components providing core functionality to the media base (col. 3 lines 17-60).

Regarding claim 14 Candelore discloses the method wherein the media base establishing the protected media path further comprises the media base selecting supplemental components

Art Unit: 2136

thereof that are to handle and operate on the content while being delivered through the protected media path, the supplemental components providing supplemental functionality to the media base (col. 6).

Regarding claim 15 Candelore discloses the method wherein the SOTA establishing trust with respect to the protected media path comprises:

the SOTA establishing trust with a policy engine of the media base (col. 4 lines 29-56);

the trusted policy engine establishing trust with every other element of the protected media path including the SITA (col. 4 lines 29-col. 5 lines 17).

Regarding claim 16 Candelore discloses the method wherein establishing trust with any element comprises receiving a proffer of an acceptable token that vouches for the element (fig. 7 element 746).

Regarding claim 17 Candelore discloses the method wherein establishing trust with any element comprises receiving a proffer of a verifiable digital certificate from an acceptable vouching authority (col. 6 lines 13-29).

Regarding claim 18 Candelore discloses the method wherein the SOTA propagating policy corresponding to the content to be delivered to the protected media path comprises:

the SOTA propagating policy to a policy engine of the media base (col. 4 lines 29-56);

the policy engine as necessary determining that each element of the protected media path including the SITA satisfies the policy (col. 4 lines 29-col. 5 lines 17).

Regarding claim 19 Candelore discloses the method wherein if the policy engine determines that a particular element of the protected media path does not satisfies the policy, the policy engine performs an action selected from a group consisting of refusing such element access to the content and preventing content from being delivered through the protected media path (fig. 7 element 726).

Regarding claim 20 Candelore discloses the method wherein the SOTA propagating policy corresponding to the content to be delivered to the protected media path comprises:

the SOTA propagating policy to a policy engine of the media base (col. 4 lines 29-56);

the policy engine propagating the policy to the SITA in the protected media path (col. 4 lines 29-col. 5 lines 17); and

the SITA as a trusted element of the protected media path abiding by such policy (col. 7 lines 40-65).

Regarding claim 21 Candelore discloses the method comprising the SOTA determining from the SITA the particular type of action to be taken with the content as delivered through the protected media path (fig. 7 element 726, and 750).

Regarding claim 22 Candelore discloses the method comprising the SOTA deciding whether the

particular type of action can be taken with the content based on the policy corresponding thereto (fig. 7 element 726, and 750 and col. 6 lines 13-29).

Regarding claim 23 Candelore discloses the method further comprising:

the SOTA obtaining the content from the source in an encrypted form, decrypting the encrypted content, and delivering the decrypted content to the media base (col. 5 lines 18-30 and col. 7 lines 23-30);

the media base processing the decrypted content as necessary and delivering the processed content to the SIAT col. 4 lines 66-col. 5 lines 64); and

the SITA encrypting the processed content and delivering the encrypted processed content to the sink (col. 7 lines 23-65).

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2136

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867.

The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

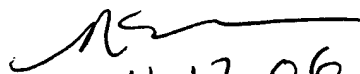
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



November 17, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


11/17/06